IN THE CLAIMS

1.   (Withdrawn) A method of implementing token-based electronic security across multiple secure web sites, in which the user has a security token, comprising:

storing unique token identification information, and the seed value of each token, in a security system;

requiring the user, upon login to a secure web site, to enter at least the code generated by the user's token;

passing the user's token code from the web site to the security system;

using the security system to verify whether or not the user's token code was generated by the user's token; and

passing the verification information from the security system to the web site, for use in web site security.

2.   (Withdrawn) The method of claim 1 wherein the requiring step further requires the user to enter a user name and user password.

3.   (Withdrawn) The method of claim 2 further comprising the step of:

the web site verifying the user name and user password before passing the user's token code to the security system.

4.   (Previously Presented) A method of accomplishing two-factor user authentication, comprising:

providing first and second user authentication methods, wherein the first and second user authentication methods are selected to authenticate at least two factors associated with the user;

enabling a user to communicate authentication data for both authentication methods to a first web site using the internet;

authenticating the user at the first web site using the first authentication method;

enabling the communication of at least some of the authentication data from the first web site to a second web site using the internet;

authenticating the user at the second web site based on the authentication data transferred

from the first web site using the second authentication method; and

wherein both web sites are involved in user authentication using the authentication data

and wherein access to content on the first web site is restricted if the user is not authenticated to

both web sites.

5.   (Previously Presented) The method of claim 4, wherein the first web site initially

authenticates the user based on the data relating to the first authentication method.

6.   (Canceled)

7.   (Previously Presented) The method of claim 5, wherein the first web site communicates

with the second web site only if the user is initially authenticated.

8.   (Previously Presented) The method of claim 7, wherein the first web site communicates

to the second web site at least data relating to the second authentication method, and user-

identification data.

9.   (Original) The method of claim 4, wherein one authentication method employs a

password.

10.   (Original) The method of claim 4, wherein one authentication method employs a token.

11.   (Original) The method of claim 10, wherein the token is hardware-based, and generates a

code that comprises at least some of the data for the authentication method.

12.   (Original) The method of claim 11, wherein the token is a stand-alone, portable device.

13.   (Original) The method of claim 11, wherein the token is USB-based and is accessed by a

browser.

Amendment Under 37 CFR 41.33(b)
Serial Number: 10/050,752
Filing Date: January 16, 2002
Title: SYSTEM AND METHOD FOR ACCOMPLISHING TWO-FACTOR USER AUTHENTICATION USING THE INTERNET

Page 4
Dkt: 105.215US1

14.   (Withdrawn) The method of claim 10, wherein the token is software-based, and generates a code that comprises at least some of the data for the authentication method.

15.   (Withdrawn) The method of claim 14, wherein the token comprises a browser plug-in.

16.   (Original) The method of claim 4, wherein one authentication method employs a fixed complex code.

17.   (Original) The method of claim 16, wherein the fixed complex code comprises a public key infrastructure.

18.   (Original) The method of claim 4, wherein one authentication method is software-based.

19.   (Original) The method of claim 4, wherein at least one user authentication method can be used across multiple web sites.

20.   (Previously Presented) The method of claim 10, wherein the token is embedded in a cell phone.

21.   (Previously Presented) A method of authenticating a user to one or more web sites, comprising:

authenticating the user to a first web site of the one or more web sites; and

once authenticated to the first web site, authenticating the user to a second web site;

wherein the user is granted access to content on the first web site only if authenticated to both the first and second web sites.

22.   (Previously Presented) The method of claim 21, wherein authenticating to the first web site is performed with a password and authentication to the second web site is performed with a token.

23.   (Previously Presented) The method of claim 21, wherein authenticating to the first web site is performed with a password and authentication to the second web site is performed with a one-time password.

24. - 27.   (Canceled)

28.   (Previously Presented) An authentication system, comprising:

one or more web sites implementing a first authentication method;

an authentication web site connected to the one or more web sites for implementing a second authentication method;

wherein authentication information for the second authentication method is entered via a first web site of the one or more web sites and transferred from the first web site to the authentication web site; and

wherein a user is granted access to content on the one or more web sites only if authenticated to both the first web site and the authentication web site.

29.   (Previously Presented) The system of claim 28, wherein the first authentication method is based on a password and the second authentication method is based on a token.

30.   (Previously Presented) The system of claim 28, wherein the first authentication method is based on a password and the second authentication method is based on a one-time password.

31. - 34.   (Canceled)